Lattice Reduction via Dense Sublattices: A Cryptanalytic No-Go

Léo Ducas[1,2] and Johanna Loyer[3]

[1] Centrum Wiskunde & Informatica, Amsterdam, The Netherlands
[2] Leiden University, Mathematical Institute, Leiden, The Netherlands
[3] Inria, Saclay, France

Abstract. Most concrete analyses of lattice reduction focus on the BKZ algorithm or its variants relying on Shortest Vector Problem (SVP) oracles. However, a variant by Li and Nguyen (Cambridge U. Press 2014) exploits more powerful oracles, namely for the Densest rank-k Sublattice Problem (DSP$_k$) for $k \geq 2$.

We first observe that, for random lattices, DSP$_2$ –and possibly even DSP$_3$– seems heuristically not much more expensive than solving SVP with the current best algorithm. We indeed argue that a densest sublattice can be found among pairs or triples of vectors produced by lattice sieving, at a negligible additional cost. This gives hope that this approach could be competitive.

We therefore proceed to a heuristic and average-case analysis of the slope of DSP$_k$-BKZ output, inspired by a theorem of Kim (Journal of Number Theory 2022) which suggests a prediction for the volume of the densest rank-k sublattice of a random lattice.

Under this heuristic, the slope for $k = 2$ or 3 appears tenuously better than that of BKZ, making this approach less effective than regular BKZ using the "Dimensions for Free" of Ducas (EUROCRYPT 2018). Furthermore, our experiments show that this heuristic is overly optimistic.

Despite the hope raised by our first observation, we therefore conclude that this approach appears to be a No-Go for cryptanalysis of generic lattice problems.

Keywords. Lattice reduction, BKZ algorithm, Dense Sublattice Problem, Post-quantum cryptography.

1 Introduction

Lattice-based cryptography is the primary platform for post-quantum cryptography. Several schemes based on the hardness of lattice problems, such as Kyber [BDK+18], Dilithium [DKL+18] or Falcon [FHK+18], have been selected by the NIST for the post-quantum standardization process. A key aspect of evaluating the security of those schemes is estimating the cost of lattice reduction.

A central tool for this task is the BKZ lattice reduction algorithm [SE94] introduced by Euchner and Schnorr. The BKZ algorithm iteratively improves a lattice basis through calls to an oracle solving the Shortest Vector Problem (SVP) on local blocks of the basis. Several variants and optimizations of BKZ have been proposed since. One notable improvement is the dimensions-for-free technique [Duc18], which allows to reduce a lattice basis for the cost of a lattice of smaller dimension. Orthogonally, Li and Nguyen [LN14] introduced a variant of BKZ in which the SVP oracle is replaced with an oracle solving the Densest

E-mail: firstname.lastname@cwi.nl (Léo Ducas), firstname.lastname@inria.fr (Johanna Loyer)

Sublattice Problem. The DSP generalizes SVP, which corresponds to its special case of searching a densest rank-1 sublattice.

In this work, we investigate the concrete cryptanalysis potential of this DSP-BKZ variant. The intuition behind it is that considering densest sublattices –rather than simply the shortest vectors– could yield better reduction of the output basis. The "quality" of the basis is essentially measured by the slope of the logarithmic norm of the Gram-Schmidt basis vectors.

We first argue that DSP_2 –or maybe even DSP_3– can be heuristically solved for the price of a lattice sieve. As this cost is only a bit larger than the best heuristic SVP algorithm [Duc18], this approach sounds promising.

We then provide theoretical predictions for the slope under the most optimistic assumptions (that the volume of dense sublattices does follow a Poisson distribution), and find out that indeed DSP_k-BKZ may provides a better slope than BKZ, but only slightly so. This gain is unfortunately not sufficient to compensate the loss of the dimensions-for-free exploited in BKZ.

Moreover, Kim [Kim22] showed that this Poissonianity assumption can not be true, but one may hope that it is not too far off. Our experiments shows on the contrary that it is very far from Poisson, with a very heavy tail, barely lighter than $O(1/x)$. In particular, the average density of the densest sublattice is significantly underestimated by the Poissonianity assumption.

We therefore conclude on a cryptanalytic No-Go for DSP-BKZ in practice in the current state of the art: the increase in cost does outweigh the potential gain of quality, even under over-optimistic assumption.

Outline of the paper. We start in section 2 with background on lattices. In Section 3, we show how to obtain a solution to DSP_2 from the output of a lattice sieve. In section 4, we provide an optimistic estimation of the expected volume of densest sublattices. In section 5 we present and analyze the variant of the BKZ algorithm based on solving the Dense Sublattice problem. Finally, in section 6 we compare our theoretical predictions with our experimental observations.

2 Preliminaries

In this section, we recall some basic notions about lattice reduction. We first introduce the notations we use in the rest of the paper.

General notations. We write vectors in lower-case bold letters and matrices in upper-case bold letters. For a vector $\mathbf{x}$, we denote $\|\mathbf{x}\|$ its ℓ_2-norm. A matrix $\mathbf{B} = (\mathbf{b}_0, \dots, \mathbf{b}_{d-1}) \in \mathbb{R}^{d\times n}$ is the matrix whose i-th column is $\mathbf{b}_i$. Logarithms are in natural base e. We denote ζ the Riemann zeta function where we fix $\zeta(1) := 1$ for notational convenience. We denote Γ the Gamma function, *i.e.*, the extension of the factorial function to real numbers. We also denote the volume of the unit ball in $\mathbb{R}^i$

$$V(i) := \frac{\pi^{i/2}}{\Gamma(i/2+1)}. \tag{1}$$

Orthogonalization. For $i = 0$ to $d-1$, we define π_i as the orthogonal projection onto the orthogonal complement of $\mathrm{Span}(\mathbf{b}_0, \dots, \mathbf{b}_{i-1})$. The Gram-Schmidt orthogonalization of the basis $\mathbf{B} = (\mathbf{b}_0, \dots, \mathbf{b}_{d-1})$ is $\mathbf{B}^\star = (\mathbf{b}_0^\star, \dots, \mathbf{b}_{d-1}^\star)$ where $\mathbf{b}_i^\star := \pi_i(\mathbf{b}_i)$. For $0 \geq i < j \leq n$, we denote by $\mathbf{B}_{[i:j]} := (\pi_i(\mathbf{b}_i), \dots, \pi_i(\mathbf{b}_j))$ the projected block from index i to j, where each vector is projected orthogonally to $\mathrm{Span}(\mathbf{b}_0, \dots, \mathbf{b}_{i-1})$. We also denote by $\mathcal{L}_{[i:j]} := \mathcal{L}(\mathbf{B}_{[i:j]})$ its corresponding local projected lattice when the basis is non-ambiguous from the context.

Lattices. Let be a basis $\mathbf{B} = (\mathbf{b}_0, \ldots, \mathbf{b}_{d-1}) \in \mathbb{R}^{d \times n}$. The lattice generated by $\mathbf{B}$ is $\mathcal{L}(\mathbf{B}) := \{\mathbf{Bx} \mid \mathbf{x} \in \mathbb{Z}^n\}$. It has dimension d and rank n, and is said 'full-rank' if $n = d$. The volume (or determinant) of lattice $\mathcal{L}$ of basis $\mathbf{B}$ is $\mathrm{Vol}(\mathcal{L}) = \prod_{i=0}^{d-1} \|\mathbf{b}_i^\star\|$. The volume is a lattice invariant since it does not change with the choice of the lattice basis. $Span(\mathbf{B})$ is the linear space spanned by the columns of $\mathbf{B}$. For a lattice $\mathcal{L} \subset \mathbb{R}^n$, a sublattice $\Lambda \subseteq \mathcal{L}$ is said primitive if and only if $\Lambda = \mathrm{Span}(\Lambda) \cap \mathcal{L}$. The minimal distance of a lattice $\mathcal{L}$ is the norm of its shortest non-zero vector and is denoted $\lambda_1(\mathcal{L})$, or simply λ_1 if $\mathcal{L}$ is clear from context.

2.1 Lattice reduction

Given a basis $\mathbf{B} = (\mathbf{b}_0, \ldots, \mathbf{b}_{d-1})$, the goal of *lattice reduction* is to find a basis of $\mathcal{L}(\mathbf{B})$ whose vectors are short and close to orthogonal from each other. This translates into flattening the slope of the sequence $(\|\mathbf{b}_i^\star\|)_i$. We define here some usual reduction notions, from the lower to higher output quality.

1. A 2-dimensional lattice basis $\mathbf{B} = (\mathbf{b}_1, \mathbf{b}_2)$ is *Lagrange reduced* if $\|\mathbf{b}_1\| = \lambda_1(\mathcal{L}(\mathbf{B}))$ and $|\langle \mathbf{b}_1, \mathbf{b}_2 \rangle| / \|\mathbf{b}_1\|^2 \leq \frac{1}{2}$.

2. A lattice basis $\mathbf{B}$ is *size-reduced* if it satisfies $\frac{|\langle \mathbf{b}_i, \mathbf{b}_j^\star \rangle|}{\|\mathbf{b}_j^\star\|^2} \leq \frac{1}{2}$ $\forall i < j \leq d$.

3. A lattice basis $\mathbf{B}$ is *LLL reduced* if it is size-reduced and satisfies $\|\mathbf{b}_i^\star\| \leq \gamma_2 \|\mathbf{b}_{i+1}^\star\|$ $\forall i \leq d$, where $\gamma_2 := \sup_{\mathcal{L}} \frac{\lambda_1(\mathcal{L})^2}{\mathrm{Vol}(\mathcal{L})^{2/n}}$ is the Hermite constant for rank 2.

4. A lattice basis $\mathbf{B}$ is BKZ_β *reduced* with block size β if it is size-reduced and satisfies $\|\mathbf{b}_i^\star\| = \lambda_1(\mathcal{L}_{[i:\min(i+\beta, d)]})$ $\forall i \leq d$.

Theorem 1 ([LLL82]). *Given* $\mathbf{B} = (\mathbf{b}_0, \ldots, \mathbf{b}_{d-1})$ *that generates a lattice* $\mathcal{L} \subset \mathbb{R}^n$*, there exists an algorithm that returns an LLL-reduced basis of* $\mathcal{L}$ *in time* $\mathrm{poly}(n, d, \log \|\mathbf{b}_i\|)$.

Note that the above statement does not require the input to be a basis. In the case of $\mathbf{B}$ being a generating set of a lattice, the LLL algorithm removes the linear dependencies and outputs a basis of the lattice. Also note that in a LLL reduced basis, any pair of consecutive vectors forms by definition a Lagrange reduced basis. Consequently, each such pair is relevant to the following lemma, often known as the "wristwatch lemma" because of its geometrical interpretation.

Lemma 1. *If a basis* $(\mathbf{b}_1, \mathbf{b}_2)$ *is Lagrange reduced, then* $\|\mathbf{b}_2^\star\| \geq \sqrt{4/3} \cdot \|\mathbf{b}_1^\star\|$.

We will come back to the BKZ algorithm [SE94] in section 2.3, but first we need some background on the Gaussian Heuristic to analyze the behavior of this algorithm.

2.2 Gaussian Heuristic

The analysis of the BKZ algorithm, and more generally of lattice reduction algorithms, often relies on heuristic assumptions. These heuristics provide approximations for the norm of shortest vector in a lattice, based on the average behavior of 'random' lattices.

2.2.1 Random lattices.

We denote $SL(n, R)$ the special linear group of degree n over a commutative ring R, *i.e.*, the set of matrices in $R^{n \times n}$ with determinant 1. Then $X_n := SL(n, \mathbb{Z}) \backslash SL(n, \mathbb{R})$ is the set of all lattices with determinant 1. We equip X_n with the measure μ_n inherited from the Haar measure of $SL(n, \mathbb{R})$, so that μ_n represents a probability measure on X_n. We denote $\mathrm{Gr}(\mathcal{L}, k)$ the set of all *primitive* rank k sublattices of the lattice $\mathcal{L}$. In the rest of the paper, when we speak about a 'random' lattice $\mathcal{L}$ of rank n and volume v, we mean sampling a unit-determinant lattice Λ as uniform in X_n, and then rescaling with the desired volume: $\mathcal{L} = v^{1/n} \cdot \Lambda$.

2.2.2 Gaussian Heuristic.

A 'naïve' version of the Gaussian Heuristic observes that for $\mathcal{S}$ the centered n-ball of radius R, the number of lattice points of norm smaller than R is about $\frac{\mathrm{Vol}(\mathcal{S})}{\mathrm{Vol}(\mathcal{L})} = \frac{R^n \cdot V(n)}{\mathrm{Vol}(\mathcal{L})}$, where $V(\cdot)$ is defined in Equation (1). Setting $\mathrm{Vol}(\mathcal{L}) \approx R^n \cdot V(n)$ gives an estimation for $\lambda_1(\mathcal{L})$, which is about $(\mathrm{Vol}(\mathcal{L})/V(n))^{1/n}$; while widely used, we will call it a naïve version of the Gaussian Heuristic. Note that this estimation only differs of a factor 2 with Minkowski upper bound, that states $\lambda_1(\mathcal{L}) \leq 2(\mathrm{Vol}(\mathcal{L})/V(n))^{1/n}$. A more precise estimation of the expected λ_1 of a random lattice was given in [Che13, Cor. 3.1.4] as a direct corollary of [Söd11].

Theorem 2 ([Söd11, Che13])**.** *Let $\mathcal{L}$ be a random n-dimensional lattice with unit volume, then*

$$\mathrm{gh}(\mathcal{L}) := \mathbb{E}_{\mathcal{L}}[\lambda_1(\mathcal{L})] = 2^{1/n}\Gamma(1+1/n) \cdot \frac{\Gamma(\frac{n}{2}+1)^{1/n}}{\sqrt{\pi}}.$$

Since $2^{1/n}\Gamma(1+1/n)$ quickly tends toward 1, the 'naïve' version mentioned above does not deviate too far from this estimation. For the rest of the paper, for any n-dimensional lattice $\mathcal{L}$, we write $\mathrm{gh}(\mathcal{L}) := \mathbb{E}_{\mathcal{L}}[\lambda_1(\mathcal{L})] = \mathrm{gh}(n) \cdot \mathrm{Vol}(\mathcal{L})^{1/n}$. Let also denote $\mathrm{lgh}(n) = \log(\mathrm{gh}(n))$.

2.2.3 Poissonianity.

Informally, the result of [Söd11] states that the points of a random lattice in a given ball resemble a Poisson point process: they occur essentially independently of each other. In particular, the number $|\mathcal{L} \cap R\mathcal{B}|$ of lattice point in a ball of radius R closely follows a Poisson distribution of parameter $\lambda = \frac{R^n \cdot V(n)}{\mathrm{Vol}(\mathcal{L})}$.

Definition 1 (Poisson distribution)**.** The Poisson distribution with parameter λ, denoted $\mathcal{P}(\lambda)$, is defined with probability $\Pr_{X \sim \mathcal{P}(\lambda)}[X = k] = \frac{\lambda^k e^{-\lambda}}{k!}$ for all $k \in \mathbb{N}$.

We recall that $\mathbb{E}[\mathcal{P}(\lambda)] = \lambda$, hence taking R following the naïve Gaussian Heuristic, we get an average of 1 point in that ball. Yet, this does not imply that this value of R is the average value of λ_1, this explains the small discrepancy between the naïve and advanced version (given as Theorem 2) of the Gaussian Heuristic for predicting λ_1.

Remark 1. While this small discrepancy has only minor quantitative consequences for predicting the shortest vector, we intend to emphasize the distinction between two notions for random processes:

1. The radius R_1 such that the expectation of the number of vectors of length less than R_1 is exactly 1
2. The average radius R before the occurrence of the first event.

Note that it is always the case that $R_1 \leq R$. For Poisson process, R is not much larger than R_1, but this is not generally the case. This is an issue we will face when attempting to predict the volume of the densest sublattice, as we only know theorems [Kim22] giving R_1 and not R. It is further stated [Kim22] that contrary to short vectors, dense sublattices *are not* Poissonian. It is therefore unclear a priori whether the heuristic derived from [Kim22] should be considered as a fair approximation, or merely as a bound.

2.3 The BKZ algorithm

The BKZ algorithm [Sch87, SE94] in its terminated form [HPS11] is used in practice for lattice reduction. It takes as input a lattice basis and a block-size β, and returns a BKZ$_\beta$-reduced basis of the lattice, *i.e.*, a basis $\mathbf{B} = (\mathbf{b}_0, \dots, \mathbf{b}_{d-1})$ satisfying $\|\mathbf{b}_i^\star\| \leq \lambda_1(\mathcal{L}_{[i:\min(i+\beta,d)]})$ for all $i \leq d$. In practice, algorithms may encounter floating-point inaccuracies during computations, so the output may not be exactly BKZ-reduced, but close.

The BKZ algorithm calls an SVP-solver on consecutive local blocks $\mathbf{B}_{[i:\min(i+\beta-1,d)]}$ for $i = 1$ to $d-1$. We assume the SVP-solver first applies standard preprocessing (such as LLL, or a stronger preprocessing) on its input basis. After each computation of the SVP-solver, the algorithm updates the current block by inserting the found vector between indices $i-1$ and i, and then LLL-reduces the updated block. The algorithm terminates when no more change occurs during an iteration. This whole process is briefly summarized in Algorithm 1. We refer the reader to the survey [AD21] for more background.

Algorithm 1: BKZ Algorithm (simplified)

```
Input: basis $\mathbf{B} = (\mathbf{b}_0, \dots, \mathbf{b}_{d-1}) \in \mathbb{R}^{n \times d}$, blocksize $\beta$
Output: a BKZ$_\beta$-reduced basis of $\mathcal{L}(\mathbf{B})$
repeat
    for $i = 0, \dots, d-2$ do
        $\mathbf{b}_i' \leftarrow \mathrm{SVP}(\mathbf{B}_{[i:\min(i+\beta,d)]})$
        $\mathbf{B} \leftarrow \mathrm{LLL}(\mathbf{b}_0, \dots, \mathbf{b}_{i-1}, \mathbf{b}_i', \mathbf{b}_i, \dots, \mathbf{b}_{d-1})$    ▷ Deletes linear dependencies
until until no change occurs;
return $\mathbf{B}$
```

We consider the *log profile* of the basis, defined as the sequence $\ell_i := \log \|\mathbf{b}_i^\star\|$ for $i = 0$ to $d-1$. The BKZ reduction flattens the decrease of the log profile as i increases. Several attempts [Sch03, BSW18] have iteratively refined the estimated behavior of the ℓ_i to better match the experimental observations.

2.3.1 Geometric Series Assumption (GSA).

Algorithm 1 outputs a modified basis $\mathbf{B} = (\mathbf{b}_0, \dots, \mathbf{b}_{d-1}) \in \mathbb{R}^{n \times d}$ with $\|\mathbf{b}_i^\star\| = \lambda_1(\mathcal{L}_{[i:\min(i+\beta,d)]})$ for $i = 0, \dots, d-\beta-1$. Let us suppose $d \gg \beta$. Then we can expect (by heuristic application of Theorem 2) $\|\mathbf{b}_i^\star\| \approx \mathrm{gh}(\mathcal{L}_{[i:i+\beta]}) = \mathrm{gh}(\beta) \cdot \mathrm{Vol}(\mathcal{L}_{[i:i+\beta]})^{1/\beta}$. Taking logarithms, gives for all i that

$$\ell_i = \log \|\mathbf{b}_i^\star\| = \mathrm{lgh}(\beta) + \frac{1}{\beta} \sum_{j=i}^{i+\beta-1} \ell_j.$$

This is a geometric series on the $\|\mathbf{b}_i^\star\|$'s. For one block of dimension β and unit volume $\mathrm{Vol}(\mathcal{L}) = 1$, we expect $\ell_i = (\beta - i - 1) \cdot \log(\alpha_\beta)$. So, for $i = 0$,

$$\begin{aligned} \ell_0 = (\beta - 1) \cdot \log(\alpha_\beta) &= \mathrm{lgh}(\beta) + \frac{1}{\beta} \sum_{j=0}^{\beta-1} \ell_j \\ &= \mathrm{lgh}(\beta) + \log(\alpha_\beta) \cdot \frac{\beta - 1}{2} \end{aligned}$$

so the slope is $\alpha_\beta = \mathrm{gh}(\beta)^{\frac{2}{\beta-1}}$. We now apply the same argument to the whole basis in dimension d with $\ell_i = (d - i - 1) \cdot \log(\alpha_\beta)$ for $i = 0, \dots, d-1$. The slope is assumed to be the same, but the first point ℓ_0 is higher. We must also take into account the volume of the lattice $\mathcal{L} = \mathcal{L}(\mathbf{B})$ with $\mathrm{gh}(\mathcal{L}) = \mathrm{gh}(d) \cdot \mathrm{Vol}(\mathcal{L})^{1/d}$. So we get

$$\frac{\|\mathbf{b}_0\|}{\mathrm{Vol}(\mathcal{L})^{1/d}} = \frac{\alpha_\beta^{d-1}}{\alpha_\beta^{(d-1)/2}} = \alpha_\beta^{(d-1)/2}$$

$$\log \|\mathbf{b}_0\| - \frac{1}{d} \log \mathrm{Vol}(\mathcal{L}) = \frac{d-1}{2} \log \alpha_\beta$$

$$\ell_0 = \log \|\mathbf{b}_0^\star\| = \log \|\mathbf{b}_0\| = \frac{d-1}{2} \log \alpha_\beta + \frac{1}{d} \log \mathrm{Vol}(\mathcal{L})$$

Hence, we get the following estimation.

Definition 2 (Geometric Series Assumption (GSA) [Sch03])**.** Let be a BKZ$_\beta$-reduced basis $\mathbf{B} = (\mathbf{b}_0, \ldots, \mathbf{b}_{d-1})$ of a lattice $\mathcal{L}$. The Geometric Series Assumption states that for $i = 1$ to d,

$$\ell_i = \log \|\mathbf{b}_i^\star\| = \left(\frac{d-1}{2} - i\right) \log \alpha_\beta + \frac{1}{d} \log \mathrm{Vol}(\mathcal{L}), \tag{2}$$

with slope $\alpha_\beta = \mathrm{gh}(\beta)^{\frac{2}{\beta-1}}$.

Remark 2. The GSA estimation matches the practical behavior of BKZ under the condition $d \gg \beta \gg 50$, but only for the coordinates from β to $d - \beta$. This ignores the behavior at the boundary coordinates, known as the *head* and the *tail.* More accurate estimations do exist [CN11, BSW18], but in this article we will stick to this simpler reasoning which is sufficient to draw our conclusions.

2.4 The Densest Sublattice problem

For an n-dimensional lattice $\mathcal{L}$ and $k \in \mathbb{N}$, let us denote by $\nu_k(\mathcal{L})$ the volume of the densest rank k sublattice in $\mathcal{L}$, *i.e.*, $\nu_k(\mathcal{L}) := \min_{A \in Gr(\mathcal{L},k)}\{\mathrm{Vol}(A)\}$.

We define the following problem, originally introduced in [GHGKN06].

Definition 3 (Densest Sublattice problem (DSP$_k$))**.** Let $k < d$, and let $\mathcal{L}$ be a d-dimensional lattice. Find a rank k sublattice $A \subset \mathcal{L}$ such that $\mathrm{Vol}(A) = \nu_k(\mathcal{L})$.

Minimizing the volume corresponds to finding a sublattice basis whose vectors are short and close to each other. The DSP problem generalizes the Shortest Vector Problem, which corresponds to the case $k = 1$. Theorem 2 provides a good approximation of $\nu_1 = \lambda_1$. In the next section, we will propose a bound on the value of ν_k for higher k, and to do so, we will make use of the following theorem.

Theorem 3 ([Thu98, Kim22])**.** *Let $H \geq 0$ and $A \in Gr(\mathcal{L}, k)$, i.e., a primitive rank k sublattices of $\mathcal{L}$. We define*

$$f_H(A) = \begin{cases} 1 \text{ if } \mathrm{Vol}(A) \leq H \\ 0 \text{ otherwise.} \end{cases}$$

Suppose $1 \leq k \leq n-1$, then

$$\int_{X_n} \sum_{A \in \mathrm{Gr}(\mathcal{L},k)} f_H(A) \, \mathrm{d}\mu_n(\mathcal{L}) = H^n \frac{1}{n} \binom{n}{k} \prod_{i=1}^{k} \frac{V(n-i+1)\zeta(i)}{V(i)\zeta(n-i+1)}$$

This theorem is a subcase of [Kim22, Theorem 3] and was previously proven in a more general form in [Thu98, Theorem 3].

3 Solving DSP_2 for the price of a Sieve

The best provable algorithm to solve DSP_k [DM13] in the worst case has complexity $k^{O(kn)}$. We here show that heuristically, we can solve DSP_2 as fast as running a sieve in dimension n. Lattice sieving algorithms [NV08, BDGL16] are designed to solve SVP, which corresponds to DSP_1. Their output is a list of lattice vectors up to a certain radius. In this section, we argue that, under standard heuristics for random lattices and sieving, this output list also suffices to identify a densest rank-2 sublattice with negligible overhead.

We rely on two standard assumptions commonly made in lattice sieving analyses:

1. *Gaussian Heuristic.* For a random unit-volume lattice of rank n one expects to find α^n many non-zero lattice vectors in the ball of radius $\alpha \cdot \mathrm{gh}(n)$.

2. *Lattice Sieving output.* We assume the sieve outputs all non-zero lattice vectors of norm at most $r = \sqrt{4/3} \cdot \mathrm{gh}(n)$.

We now argue that the densest rank 2 sublattice has volume at most $\mathrm{gh}(n)^2$. Let $\mathbf{x} \in L$ be a shortest vector, with norm $\|\mathbf{x}\| = \mathrm{gh}(n)$ by Gaussian Heuristic, and let $\mathbf{y} \in L$ be such that the projection $\pi_{\mathbf{x}}^{\perp}(\mathbf{y})$ is a shortest vector of the projected lattice $\pi_{\mathbf{x}}^{\perp}(L)$. The lattice $\pi_{\mathbf{x}}^{\perp}(L)$ has rank $n-1$ and volume $1/\|\mathbf{x}\|$, hence we expect $\|\pi_{\mathbf{x}}^{\perp}(\mathbf{y})\| = \frac{\mathrm{gh}(n-1)}{\mathrm{gh}(n)^{1/n}} \leq \mathrm{gh}(n)$ where the inequality holds for large enough n. Thus the lattice generated by $\mathbf{x}$ and $\mathbf{y}$ has volume $\|\mathbf{x}\| \cdot \|\pi_{\mathbf{x}}^{\perp}(\mathbf{y})\| \leq \mathrm{gh}(n)^2$.

Since every rank-2 lattice admits a Lagrange-reduced basis, we only need to search through pairs $\mathbf{x}, \mathbf{y}$ such that $\langle \mathbf{x}, \mathbf{y} \rangle \leq \|\mathbf{x}\| \cdot \|\mathbf{y}\|/2$, *i.e.*, pairs of vectors at angle of at least $\pi/3$. The determinant of the lattice generated by such a pair $\mathbf{x}, \mathbf{y}$ is $\sqrt{\|\mathbf{x}\|^2 \cdot \|\mathbf{y}\|^2 - \langle \mathbf{x}, \mathbf{y} \rangle^2} \geq \sqrt{3/4} \cdot \|\mathbf{x}\| \cdot \|\mathbf{y}\|$. Because $\|\mathbf{x}\|, \|\mathbf{y}\| \geq \mathrm{gh}(n)$, a reduced pair generating the densest sublattice must satisfy $\|\mathbf{x}\|, \|\mathbf{y}\| \leq \sqrt{4/3} \cdot \mathrm{gh}(n)$. Hence, such a pair can be found among the output list of the sieve.

Let $\mathbf{v}_1, \ldots, \mathbf{v}_N$ denote the $N = (4/3)^{n/2}$ shortest vectors, sorted by increasing norm. Rephrasing the Gaussian Heuristic, we expect $\|\mathbf{v}_i\| = i^{1/n} \cdot \mathrm{gh}(n)$. So for $\mathbf{x} = \mathbf{v}_i$ and $\mathbf{y} = \mathbf{v}_j$, we have $\|\mathbf{x}\| \cdot \|\mathbf{y}\| = (ij)^{1/n} \cdot \mathrm{gh}(n)^2$. To satisfy $\|\mathbf{x}\| \cdot \|\mathbf{y}\| \leq \sqrt{4/3} \cdot \mathrm{gh}(n)^2$, it is necessary that $ij \leq (4/3)^{n/2} = N$. This means that for each $i \geq 1$ we only need to test $\mathbf{v}_j$'s up to $j \leq N/i$. As the $\mathbf{v}_i$ vectors are already sorted by length, the total number of pairs to check is:

$$\sum_{i=1}^{N} \frac{N}{i} \approx N \ln(N).$$

On the other hand, the best known sieve [NV08, BDGL16] have complexity N^c for a constant $c > 1$, hence the cost of heuristically solving DSP_2 for random lattices is dominated by the cost of sieving.

Given how much margin there is compared to the complexity of [BDGL16] one may want to explore applying the configuration strategy [HK17] to solve DSP_3 still for the same price. However, given the negative results from the following sections, this effort appears rather vain.

4 Assumption on the volume of densest sublattice

Later in section 5, we analyse our variant of BKZ that uses DSP oracle. To do so, we require a bound on the volume of densest sublattices, denoted ν_k, where k is the rank of the densest sublattice we are searching. We introduce the following value.

Definition 4. For $k \leq n$, define

$$\mathrm{h}_k(n) := \left(\frac{n}{\binom{n}{k}} \prod_{i=1}^{k} \frac{V(i)\zeta(n-i+1)}{V(n-i+1)\zeta(i)} \right)^{\frac{1}{n}} \tag{3}$$

We now state a probabilistic lower bound on ν_k.

Theorem 4. *Let $k \geq n$, $\mathcal{L}$ a random n-dimensional lattice, and $\varepsilon \in (0,1)$. Then with probability $1-\varepsilon$,*

$$\nu_k(\mathcal{L}) \geq \varepsilon^{1/n} \cdot \mathrm{h}_k(n) \cdot \mathrm{Vol}(\mathcal{L})^{1/n}.$$

Proof. Suppose $\mathrm{Vol}(\mathcal{L}) = 1$. For $H > 0$, define $N_H(\mathcal{L}) := \sum_{A \in Gr(\mathcal{L},k)} f_H(A)$ as the number of primitive rank-k sublattices of $\mathcal{L}$ with volume at most H. Since $\mathcal{L}$ contains no such sublattice with volume less than $\nu_k(\mathcal{L})$, we have by definition of N_H, $\Pr_{\mathcal{L}}[\nu_k(\mathcal{L}) > H] = \Pr[N_H(\mathcal{L}) = 0] = 1 - \Pr[N_H(\mathcal{L}) \geq 1]$. Markov's inequality[1] implies $\Pr_{\mathcal{L}}[N_H(\mathcal{L}) \geq 1] \leq \mathbb{E}_{\mathcal{L}}[N_H(\mathcal{L})]$. Hence, $\Pr_{\mathcal{L}}[\nu_k(\mathcal{L}) > H] \geq 1 - \mathbb{E}_{\mathcal{L}}[N_H(\mathcal{L})] = 1 - H^n \frac{1}{n} \binom{n}{k} \prod_{i=1}^{k} \frac{V(n-i+1)\zeta(i)}{V(i)\zeta(n-i+1)}$ by Theorem 3. Let be $\varepsilon \in (0,1)$. Taking $H = \mathrm{h}_k(n)$ as in Definition 4 yields to $\Pr_{\mathcal{L}}[\nu_k(\mathcal{L}) \geq \varepsilon^{1/n} H] \geq 1 - \varepsilon$. Rescaling with $\mathrm{Vol}(\mathcal{L})$ completes the proof. □

Remark 3. The factor $\varepsilon^{1/n}$ quickly converges towards 1 even for small ε. For example, setting $\varepsilon = 2/n$ and $n \geq 5$ implies $\nu_k(\mathcal{L}) \geq 0.8 \cdot \mathrm{h}_k(n) \cdot \mathrm{Vol}(\mathcal{L})^{1/n}$ with high probability $1 - o(1)$.

As a direct application in case $k = 1$, we obtain:

Corollary 1. *Let $\mathcal{L}$ be a random n-dimensional lattice $\mathcal{L}$ and $\varepsilon \in (0,1)$. Then, with probability $1-\varepsilon$, we have $\lambda_1(\mathcal{L}) \geq \varepsilon^{1/n} \cdot \mathrm{h}_1(n) \cdot \mathrm{Vol}(\mathcal{L})^{1/n}$, where*

$$\mathrm{h}_1(n) := \left(\frac{V(1)\zeta(n)}{V(n)} \right)^{1/n} = \frac{2^{1/n}}{\sqrt{\pi}} \Gamma(n/2+1)^{1/n} \cdot \zeta(n)^{1/n}.$$

Recall the Gaussian Heuristic as stated in theorem 2:

$$\mathrm{gh}(n) = \mathbb{E}_{\mathcal{L}}[\lambda_1(\mathcal{L})] = \frac{2^{1/n}}{\sqrt{\pi}} \Gamma(n/2+1)^{1/n} \cdot \Gamma(1+1/n).$$

The two expressions for λ_1 are overwhelmingly close to each other, as the only mismatch $\zeta^{1/n}/\Gamma(1+1/n)$ rapidly converges to 1 from above as n increases.

Our corollary provides a *probabilistic lower bound*, hence it gives the most optimistic value one can expect, while the Gaussian Heuristic comes from a mean value and the concentration of the probability density around it due to Poissonianity. So, for case $k = 1$, the literature indistinctly writes 'Gaussian Heuristic' to refer to the lower bound, the mean value, and the heuristic that those values correspond to the real behavior of random lattices, as well as the behavior of lattices handled in reduction algorithms.

However, when $k > 1$, we do not have the luxury of mixing these different notions as they no longer coincide. More particularly, the distribution of ν_k is not Poissonian [Kim22], so we cannot claim about the concentration around this heuristic value. Thus, we will adopt the most optimistic estimation to draw negative results in later sections.

Definition 5 (Heuristic)**.** For $\mathcal{L}$ a n-dimensional random lattice, $\nu_k(\mathcal{L}) \approx \mathrm{h}_k(\mathcal{L}) \cdot \mathrm{Vol}(\mathcal{L})^{1/n}$, where h_k is defined in definition 4.

[1] Markov inequality: For $a > 0$ and X a nonnegative random variable, $\Pr[X \geq a] \leq \mathbb{E}[X]/a$.

5 A variant of BKZ algorithm using Dense Sublattice Problem oracle

An extension of the BKZ algorithm has been suggested by [GHGKN06] and then formalized by [LN14]. The idea is to replace the SVP oracle with a DSP oracle. By doing so, the algorithm may not necessarily find the shortest vector at each iteration, but overall it yields a reduction of better quality. This motivates the introduction of a reduction notion that accounts the volume of the densest sublattices. [GHGKN06] introduces the Rankin reduction[2]. A basis $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ of an n-dimensional lattice $\mathcal{L}$ is said k-Rankin reduced if its first k vectors satisfy $\mathrm{Vol}(\mathbf{b}_1, \dots, \mathbf{b}_k) = \nu_k(\mathcal{L})$. Moving into a Rankin-reduction block by block, we define below the notion of DSP-BKZ reduction. Note that Li and Nguyen introduced a similar definition of reduction, called Block-Rankin reduction, but their definition considers conditions on both primal and dual, while only the primal matter to us here.

Definition 6 (DSP-BKZ$_{\beta,k}$ reduction)**.** A lattice basis $\mathbf{B} = (\mathbf{b}_0, \dots, \mathbf{b}_{d-1})$ with $\mathbf{b}_i \in \mathbb{R}^n$ is said to be DSP-BKZ$_{\beta,k}$-reduced with block-size β and dimension k if

$$\prod_{j=ik}^{(i+1)k-1} \|\mathbf{b}_j^\star\| = \nu_k(\mathcal{L}_{[ik:\min(ik+\beta,d)]})$$

for all $i = 1, \dots, \lfloor d/k \rfloor$. This means that each lattice generated by k consecutive $\mathbf{b}_i$ is the densest rank-k sublattice of the block of size β.

DSP oracle. As said in Section 3, sieving algorithms can easily be used to construct a DSP-2 solver. Within our algorithm, any DSP-solver can be inserted as a brick. We also assume, for simplicity, that the DSP oracle operates standard preprocessing on its input basis.

5.1 The DSP-BKZ algorithm.

Li and Nguyen described a variant of the BKZ algorithm with DSP oracles [LN14, Algorithm 3]. In Algorithm 2 we summarize the part of their algorithm that concerns the DSP-BKZ reduction of the basis.

Algorithm 2: DSP-BKZ Algorithm [LN14, Algorithm 3] (simplified)

```
  Input: basis $\mathbf{B} = (\mathbf{b}_0, \dots, \mathbf{b}_{d-1}) \in \mathbb{R}^{n \times d}$, blocksize $\beta$, rank $k$
  Output: a DSP-BKZ$_{\beta,k}$-reduced basis of $\mathcal{L}(\mathbf{B})$
1 repeat
2     for $i = 0, \dots, \lfloor \frac{d}{k} \rfloor - 1$ do
3         $\mathbf{b}'_{ik}, \dots, \mathbf{b}'_{(i+1)k-1} \leftarrow \mathrm{DSP}_k(\mathbf{B}_{[ik:ik+\beta]})$
4         $\mathbf{B} \leftarrow \mathcal{L}L(\mathbf{b}_0, \dots, \mathbf{b}_{ik-1}, \mathbf{b}'_{ik}, \dots, \mathbf{b}'_{(i+1)k-1}, \mathbf{b}_{ik}, \dots, \mathbf{b}_{(i+1)k-1}, \mathbf{b}_{(i+1)k}, \dots, \mathbf{b}_{\min(ik+\beta,d)-1})$
5 until until no change occurs;
6 return $\mathbf{B}$
```

Step 3 ensures that $\mathbf{b}'_{ik}, \dots, \mathbf{b}'_{(i+1)k-1}$ satisfy $\prod_{j=ik}^{(i+1)k-1} \|\pi_j(\mathbf{b}'_j)\| = \nu_k(\mathcal{L}_{[ik:ik+\beta]})$. Step 4 replaces a block in $\mathbf{B}$ and uses the ability of LLL algorithm for clean up linear dependencies in order and restore a basis of the lattice.

[2] This reduction is named after the Rankin invariant [Ran53], namely the value $\gamma_{n,k}(\mathcal{L}) := (\nu_k(\mathcal{L})/\mathrm{Vol}(\mathcal{L})^{k/n})^2$ that is the Rankin invariant of lattice $\mathcal{L}$.

We now aim to derive a GSA-style (see Section 2.3.1) prediction for the log-profile $\ell_i := \|\mathbf{b}_i^\star\|$ of a DSP-BKZ reduced basis, under Definition 5. Let be $d, \beta \in k\mathbb{N}$ for simplicity, and let us suppose $d \gg \beta$. By definition, a DSP-BKZ$_{\beta,k}$ reduced basis satisfies:

$$\prod_{j=ik}^{ik+\beta-1} \|\mathbf{b}_j^\star\| = \nu_k(\mathcal{L}_{[ik:ik+\beta]}) \approx \mathrm{h}_k(\beta) \cdot \mathrm{Vol}(\mathcal{L}_{[ik:ik+\beta]})^{k/\beta}$$

where we apply our bound on ν_k from section 4. We write with equality from now on for simplicity of the notation. Taking the log gives

$$\ell'_i := \sum_{j=ik}^{(i+1)k-1} \ell_j = \log \mathrm{h}_k(\beta) + \frac{k}{\beta} \sum_{j=ik}^{ik+\beta-1} \ell_j = \log \mathrm{h}_k(\beta) + \frac{k}{\beta} \sum_{j=i}^{i+\frac{\beta}{k}-1} \ell'_j.$$

This linear recurrence implies a geometric series in i for the volumes $\prod_{j=ik}^{(i+1)k-1} \|\mathbf{b}_j^\star\|$. Considering one block of dimension β and unit volume, we expect $\ell'_i = (\frac{\beta}{k} - i - 1)\log \alpha'_\beta$ for $i = 0, \ldots, \frac{\beta}{k} - 1$, for some slope α'_β to be determined. For $i = 0$, we have

$$\begin{aligned} \ell'_0 &= \log \mathrm{h}_k(\beta) + \frac{k}{\beta} \sum_{j=0}^{\beta/k-1} \ell'_j \\ (\beta/k - 1)\log \alpha'_\beta &= \log \mathrm{h}_k(\beta) + \frac{\beta/k - 1}{2} \log \alpha'_\beta \\ \frac{\beta/k - 1}{2} \log \alpha'_\beta &= \log \mathrm{h}_k(\beta) \end{aligned}$$

so the slope of the ℓ'_i is $\alpha'_\beta = \mathrm{h}_k(\beta)^{\frac{2k}{\beta - k}}$. We apply the same argument to a basis in dimension d with $\ell'_i = (d/k - i - 1)\log \alpha'_\beta$ for $i = 0, \ldots, \frac{d}{k} - 1$. We have

$$\begin{aligned} \log \mathrm{Vol}(\mathcal{L}) &= \sum_{j=0}^{d/k-1} \ell'_j = \sum_{j=0}^{d/k-1} (d/k - 1 - j)\log \alpha'_\beta \\ &= \log(\alpha'_\beta) \frac{1}{2k}(d/k - 1) \cdot d \end{aligned}$$

So $\ell'_0 - \frac{1}{d}\log \mathrm{Vol}(\mathcal{L}) = (1 - \frac{1}{2k})(d/k - 1)\log \alpha'_\beta$. Hence,

$$\ell'_i = [(1 - 1/2k)(d/k - 1) - i] \log \alpha'_\beta + \frac{1}{d} \log \mathrm{Vol}(\mathcal{L})$$

We now have to recover the ℓ_i from the sums ℓ'_i.

Lemma 1 states $\ell_{ik+j} \geq \ell_{ik} - j \log \sqrt{4/3}$. Summing on j gives $\ell'_i = \sum_{j=0}^{k-1} \ell_{ik+j} \geq \sum_{j=0}^{k-1} (\ell_{ik} - j \log \sqrt{4/3}) = k\ell_{ik} - \frac{k(k-1)}{2} \log \sqrt{4/3}$. So $\ell'_i = \sum_{j=0}^{k-1} \ell_{ik+j} \leq k(\ell_{ik} - k \log \sqrt{4/3})$. Hence

$$\ell_{ik} \geq \frac{\ell'_i}{k} + k^2 \log \sqrt{4/3} \tag{4}$$

Let us now rewrite with some $m = ik + j$ where $i = \lfloor \frac{m}{k} \rfloor = m//k$ and $j = m - \lfloor \frac{m}{k} \rfloor k = m\%k < k$). We have $\ell_m = \ell_{ik+j} \geq \ell_{ik} + j \log \sqrt{4/3}$.

$$\ell_m \geq \frac{1}{k}\left[(1 - 1/2k)(d/k - 1) - \lfloor \frac{m}{k} \rfloor\right] \log \alpha'_\beta + \frac{1}{kd} \log \mathrm{Vol}(\mathcal{L}) + (m - \lfloor \frac{m}{k} \rfloor k) \cdot k \log \sqrt{4/3} \tag{5}$$

$$\geq \frac{1}{k^2}\left[(k - 1/2)(d/k - 1) - m\right] \log \alpha'_\beta + \frac{1}{kd} \log \mathrm{Vol}(\mathcal{L}) \tag{6}$$

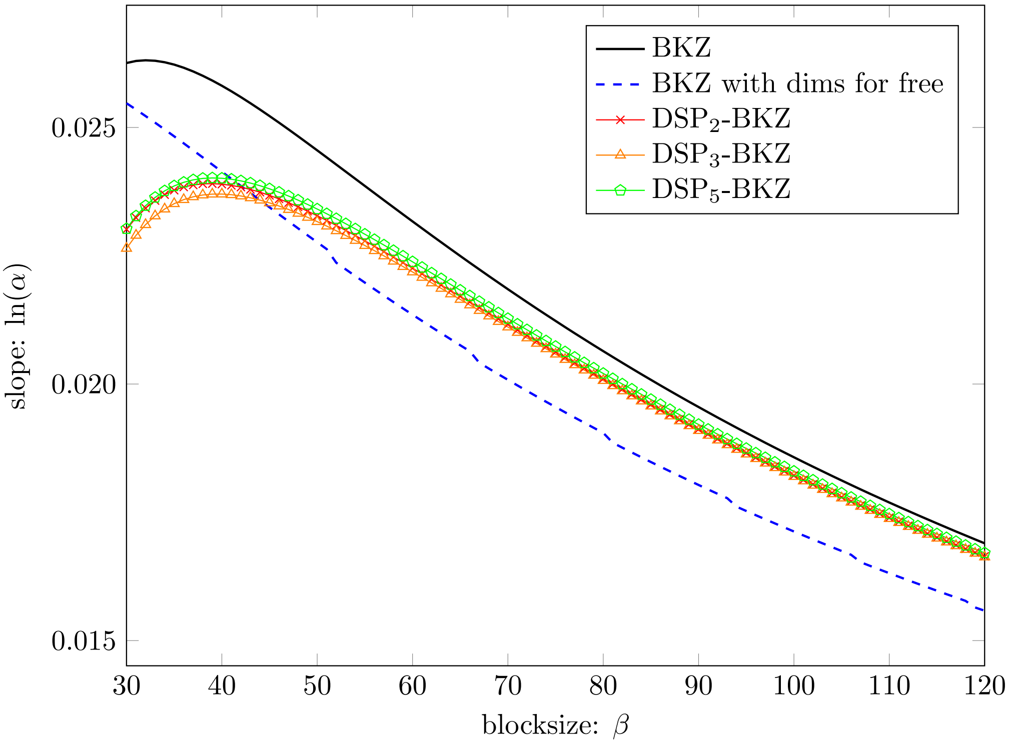


Figure 1: Simulated slopes α_β in function of block size β, for each of the considered reduction algorithms.

We get the following prediction.

Definition 7 (Prediction for DSP-BKZ$_{\beta,k}$-reduced basis)**.** Let be a DSP-BKZ$_{\beta,k}$ reduced basis $\mathbf{B} = (\mathbf{b}_0, \ldots, \mathbf{b}_{d-1})$ of a lattice $\mathcal{L}$. Our prediction based on the Geometric Series Assumption, along with the assumption that $\nu_k(\mathcal{L}) = \mathrm{h}_k(\mathcal{L})$, states that $\forall i = 1, \ldots, d$:

$$\ell_i = \frac{1}{k^2}\left[(k-1/2)(d/k-1) - i\right] \log \alpha'_\beta + \frac{1}{kd} \log \mathrm{Vol}(\mathcal{L})$$

with slope $\alpha_\beta = (\alpha'_\beta)^{1/k^2} = \mathrm{h}_k(\beta)^{\frac{2}{k(\beta-k)}}$.

Remark 4. As for GSA, this ignores what happens for the first and last coordinates, which will certainly deviate from this prediction.

6 Experimental results

6.1 Simulation of the slopes of DSP-BKZ$_{\beta,k}$ reduced basis.

In section 5, we analytically predicted the slope behavior of a DSP-BKZ reduced basis. This prediction relies on an optimistic estimate of the volume of the densest rank-k sublattice ν_k, approximated by h_k, taken at the limit of its lower bound from theorem 4.

We have run simulations for our DSP-BKZ$_{\beta,k}$ algorithm for different choices of k and compared it with the state-of-the-art dimensions-for-free technique [Duc18]. Figure 1 plots the logarithm of the slope α_β as a function of the block size β. Recall that lower slope values indicate better basis reduction.

A first observation is that taking the algorithm parameter $k > 1$ improves the slope compared to BKZ, but then increasing it again only slightly improves the slope at $k = 3$, but then the trend reverses and the slope increases. We first observe that taking the DSP-BKZ parameter $k > 1$ improves the slope compared to the original BKZ. Setting $k = 3$ slightly improves the slope, but increasing k further degrades the quality of the reduction.

The state-of-the-art dimensions-for-free algorithm [Duc18] uses a trick to reduce the cost as if the dimension were only $n - \frac{n\ln(4/3)}{\ln(n/2\pi e)}$ instead of n, shifting the BKZ curve to the left. As a result, it outperforms DSP-BKZ for block sizes $\beta \gtrsim 40$.

As a negative result, the dim-for-free algorithm outperforms ours for block sizes $\beta \gtrsim 40$. When β is small, the predictions are less accurate, and we shall not forget that the real behavior of our algorithm would be worse than our optimistic prediction. We conclude that the densest sublattices seem in fact not dense enough to provide a significant advantage over existing techniques such as dimension-for-free BKZ.

6.2 On the Poissonianity of dense sublattices.

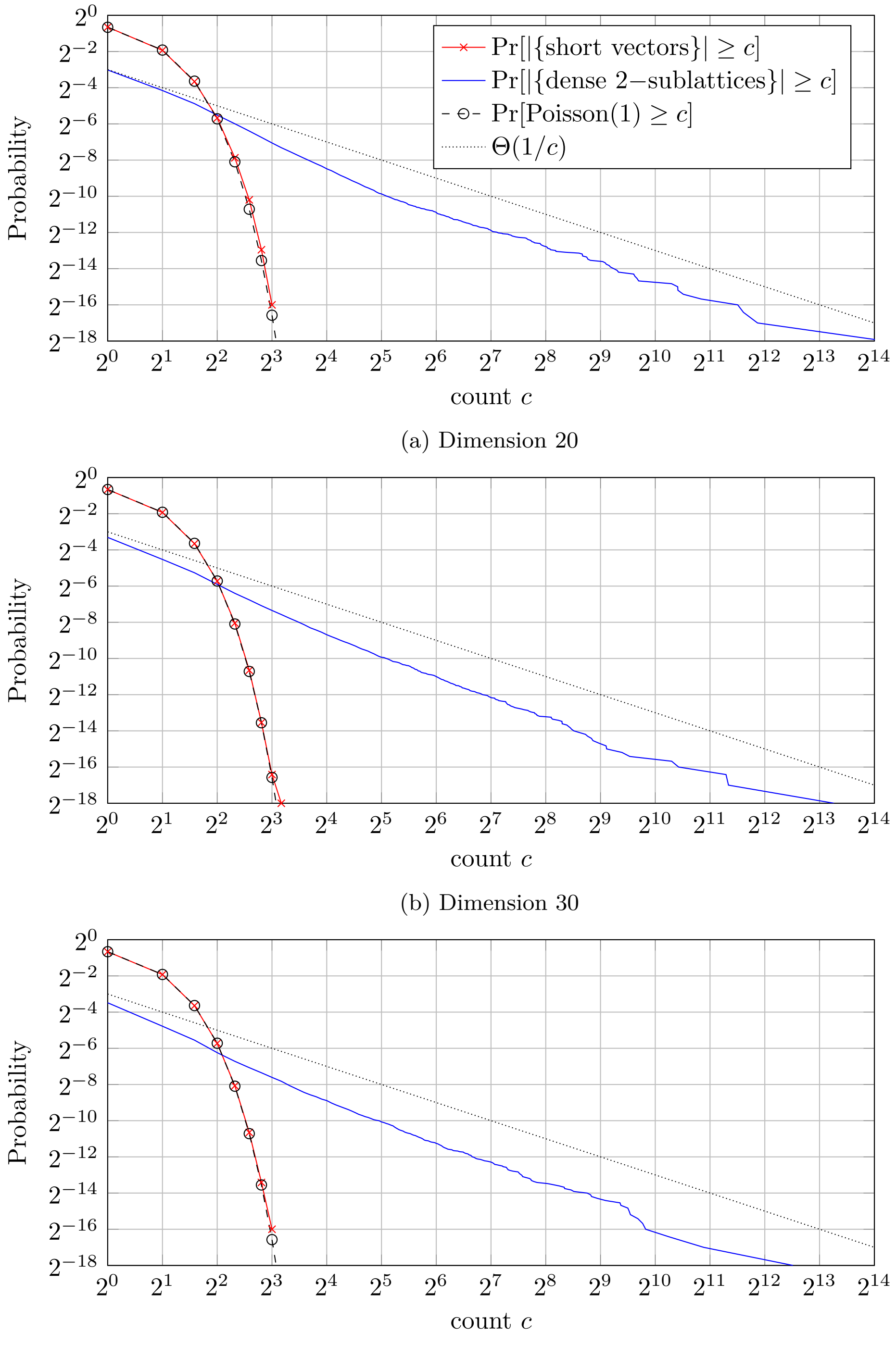
Let be a random lattice $\mathcal{L}$ with unit volume. Figure 2 plots the number of dense primitive rank k sublattices of volume smaller than $\mathrm{h}_k(n)$, for $k = 1$, and $k = 2$. By short vectors, we mean vectors of shorter than $\mathrm{h}_1(n)$, and by dense 2-sublattice, we mean denser than $\mathrm{h}_2(n)$

The figure also plots the theoretical Poisson distribution $\mathcal{P}(1)$ for comparison. The Poisson parameter is the mean value of this number, given by theorem 3: $H = h_k(n)$, the mean value of the number of such sublattices is $(H/h_k(n))^n = 1$.

Figure 2 confirms, if it ever were to be doubted, that the number of short vectors indeeds follows a poisson distribution, as asymptotically proven in [Söd11]. We further note that this prediction is already extremely accurate in dimensions as small at 20.

On the contrary, the number of dense sublattices is visibly far from a Poisson distribution, as formally proved by [Kim22]. We further note a very heavy tail, apparently decreasing as $\Theta(1/c^{\alpha})$ for some α barely larger than 1.

This is a serious obstacle to obtaining good cryptanalytic performance from a DSP-BKZ algorithms: this means that the improvements Figure 1 of DSP-BKZ over BKZ are likely overestimated. Indeed, such a heavy tail means that dense sublattices tend to come in large bunches, but that most of the time their are none. This is visible on the left side of the plots of 2: a dense sublattice exists for less than 1/10 random lattices in those dimensions, while a short vector exists with probability greater than 1/2. This increases the average volume of the densest sublattice compared to the prediction given by $\mathrm{h}_2(n)$, and thus worsens the slope.



(a) Dimension 20

(b) Dimension 30

(c) Dimension 40

Figure 2: Distribution of the number of short vectors and dense 2-sublattices, compared to the Poisson distribution.

References

[AD21] Martin Albrecht and Léo Ducas. Lattice attacks on ntru and lwe: a history of refinements. *Cryptology ePrint Archive*, 2021. doi:10.1017/9781108854207.004.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In *Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete algorithms*, pages 10–24. SIAM, 2016. doi:10.1137/1.9781611974331.ch2.

[BDK$^+$18] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-kyber: a cca-secure module-lattice-based kem. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367. IEEE, 2018. doi:10.1109/EuroSP.2018.00032.

[BSW18] Shi Bai, Damien Stehlé, and Weiqiang Wen. Measuring, simulating and exploiting the head concavity phenomenon in bkz. pages 369–404, 2018. doi:10.1007/978-3-030-03326-2_13.

[Che13] Yuanmi Chen. Lattice reduction and concrete security of fully homomorphic encryption (ph. d. thesis), 2013.

[CN11] Yuanmi Chen and Phong Q Nguyen. Bkz 2.0: Better lattice security estimates. pages 1–20, 2011. doi:10.1007/978-3-642-25385-0_1.

[DKL$^+$18] Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 238–268, 2018. doi:10.13154/tches.v2018.i1.238-268.

[DM13] Daniel Dadush and Daniele Micciancio. Algorithms for the densest sub-lattice problem. pages 1103–1122, 2013. doi:10.1137/1.9781611973105.79.

[Duc18] Léo Ducas. Shortest vector from lattice sieving: a few dimensions for free. pages 125–145, 2018. doi:10.1007/978-3-319-78381-9_5.

[FHK$^+$18] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang, et al. Falcon: Fast-fourier lattice-based compact signatures over ntru. *Submission to the NISTâ€™s post-quantum cryptography standardization process*, 36(5):1–75, 2018. URL: https://www.di.ens.fr/~prest/Publications/falcon.pdf.

[GHGKN06] Nicolas Gama, Nick Howgrave-Graham, Henrik Koy, and Phong Q Nguyen. Rankin's constant and blockwise lattice reduction. In *Annual International Cryptology Conference*, pages 112–130. Springer, 2006. doi:10.1007/11818175_7.

[HK17] Gottfried Herold and Elena Kirshanova. Improved algorithms for the approximate k-list problem in euclidean norm. pages 16–40, 2017. doi:10.1007/978-3-662-54365-8_2.

[HPS11] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. pages 447–464, 2011. doi:10.1007/978-3-642-22792-9_25.

[Kim22] Seungki Kim. Mean value formulas on sublattices and flags of the random lattice. *Journal of Number Theory*, 241:330–351, 2022. doi:10.1016/j.jnt.2022.03.013.

[LLL82] Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Matematische Annalen*, 1982. doi:10.1007/BF01457454.

[LN14] Jianwei Li and Phong Q Nguyen. Approximating the densest sublattice from rankin's inequality. *LMS Journal of Computation and Mathematics*, 17(A):92–111, 2014. doi:10.1112/S1461157014000333.

[NV08] Phong Q Nguyen and Thomas Vidick. Sieve algorithms for the shortest vector problem are practical. *Journal of Mathematical Cryptology*, 2(2):181–207, 2008. doi:10.1515/JMC.2008.009.

[Ran53] Robert Alexander Rankin. On positive definite quadratic forms. *Journal of the London Mathematical Society*, 1(3):309–314, 1953. doi:10.1112/jlms/s1-28.3.309.

[Sch87] Claus-Peter Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical computer science*, 53(2-3):201–224, 1987. doi:10.1016/0304-3975(87)90064-8.

[Sch03] Claus Peter Schnorr. Lattice reduction by random sampling and birthday methods. pages 145–156, 2003. doi:10.1007/3-540-36494-3_14.

[SE94] Claus-Peter Schnorr and Martin Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Mathematical programming*, 66:181–199, 1994. doi:10.1007/BF01581144.

[Söd11] Anders Södergren. On the poisson distribution of lengths of lattice vectors in a random lattice. *Mathematische Zeitschrift*, 269(3):945–954, 2011. doi:10.1007/s00209-010-0772-8.

[Thu98] Jeffrey Lin Thunder. Higher-dimensional analogs of hermite's constant. *Michigan Mathematical Journal*, 45(2):301–314, 1998. doi:10.1307/mmj/1030132184.